KuppingerCole Report

WHITEPAPER

By Alejandro Leal
June 23, 2022

Customer authentication with zero-friction passwordless authentication

To increase security and convenience, businesses and organizations need to adopt and implement a modern authentication system that does not rely on customers remembering usernames and passwords. Beyond Identity's newest product, Secure Customers, is a secure and frictionless authentication solution. Its invisible passwordless multi-factor authentication (MFA) makes credential-based attacks and account takeover fraud extremely difficult to execute by fully eliminating the password and improving user experience at the same time.

By **Alejandro Leal**

Content

Commissioned by BEYOND IDENTITY

1 Introduction / Executive Summary

Digital identity is at the heart of every organization's digital transformation. In essence, digital transformation is commonly regarded as an implementation or process that organizations go through to make better use of emerging technologies in response to employee or customer expectations. If digital transformation is a response to the changing business landscape, digital identity has become the foundation of the digital economy.

As a result, businesses and organizations need Identity and Access Management (IAM) solutions to manage digital identities as they access applications, data, and resources. Traditional IAM systems were designed from the point of view that an enterprise provisions and manages all the identities of employees. Most organizations have IAM products in place already. However, many are finding that their current solutions are not able to meet customer expectations or security requirements.

In order to deter fraud, comply with new regional and industry-specific regulations, and improve customer experiences, organizations are adopting Consumer Identity and Access Management (CIAM) solutions. CIAM is a parallel to traditional IAM that has become a substantial market of its own. While the market continues to grow, many vendors are offering mature solutions with standard and deluxe features to serve millions of users across all sectors.

CIAM has diverged from traditional IAM in supporting some baseline features for analyzing customer behavior, as well as collecting consent for user data usage and securely storing data for those users. Unlike IAM systems which handle hundreds of thousands of users with complex access control use cases, some CIAM systems can store billions of user identities and undertake hundreds of millions of login processes.

Organizations must find new ways to assess and manage security risks while remaining secure and compliant without causing disruptions to their customers and business operations.

By providing a transparent and secure digital experience at every stage of the customer lifecycle, CIAM solutions can help companies acquire customers faster, manage their identities, enhance user experience, and improve scalability. Essentially, CIAM systems are designed to provision, authenticate, authorize, collect, and store information about consumers from across many domains.

Therefore, CIAM is a real differentiator that can help businesses grow through the process of digital transformation by providing better consumer experiences, strengthening data privacy, and increasing security. Although CIAM systems generally use weak password-based authentication, they also support social logins and other more robust authentication methods. Yet existing solutions for customer authentication do not eliminate the source of friction and security risk - the password.

Organizations often face high maintenance costs if they rely on passwords for customer authentication. Not only is password authentication insecure, but it is also inconvenient for customers and expensive to maintain. Since password elimination is recognized as a fundamental goal for the IT security industry, passwordless options are increasingly gaining popularity and widespread adoption.

In recent years, credential-based attacks and account takeover fraud cases have been on the rise, which have disrupted businesses and organizations already overstretched by the COVID-19 pandemic. By removing the risk associated with passwords, however, organizations could prevent password-based threats while increasing the overall security posture of their organizations.

Therefore, organizations need to innovate their authentication methods, eliminate passwords, and implement an approach that is scalable, secure, and user-friendly. As a result of getting rid of passwords, organizations will be able to adopt and implement a modern authentication system that does not rely on users remembering passwords; thus, simultaneously increasing security and convenience.

By removing passwords and other phishable factors, Beyond Identity provides Secure Customers, which is a secure and frictionless authentication solution. Its invisible passwordless multi-factor authentication (MFA) enables companies to secure access to applications and critical data with dynamic risk-based access decisions, make credential-based attacks and account takeover fraud extremely difficult to execute by fully eliminating the password, and dramatically improve the user experience with no need for one-time passcodes (OTP), push notifications, or second devices.

2 Highlights

- Despite the increase of CIAM products in the market, passwords remain the source of friction and security risk for customer authentication solutions.
- Traditional MFA solutions were supposed to reduce phishing and ransomware attacks, but these solutions still rely on a password as the first factor of authentication and second factors continue to be bypassed by attackers- and, not to mention, frustrate legitimate customers.
- Businesses and organizations must be able to identify their customers from fraudsters or they may not only suffer financial losses, but also lose their customers' trust in the long run.
- Passwordless solutions that support risk-based authentication provide the ability to continuously validate and ensure that each device is registered to a known and authorized user and ensure that it meets the security requirements of the organization and the attempted action.
- Beyond Identity offers a passwordless solution that provides customers with strong, unphishable MFA without user friction by eliminating the password and securing access to applications and critical data with dynamic risk-based access decisions that makes credential-based attacks and account takeover fraud difficult to execute.

3 Fraud - Account Takeover and Other Types

Since the root cause of most account takeover fraud and other password-based threats such as social engineering attacks and SIM swaps is the password, many companies have tried to mitigate account takeover risks with band-aid solutions such as password-based MFA. Nevertheless, as long as the password continues to exist, attackers will find a way to breach and compromise customer accounts.

Fraud is a major cost to businesses worldwide. As a result of the COVID-19 pandemic, businesses and organizations have become more susceptible to account takeover and other types of fraud. Personal information such as email addresses, passwords, credit card numbers, and social security numbers can easily be stolen by fraud perpetrators for financial gain.

Consequently, companies of all industries face the same challenge: the complex and constantly changing world of fraud detection. Cybersecurity Ventures estimates that cybercrime costs will reach \$10.5 trillion by 2025. Banking, finance, payment services, and retail are some of the most frequent targets for fraudsters, as expected. To make matters worse, fraud perpetrators are continuously diversifying and innovating their Tactics, Techniques, and Procedures (TTPs).

The most prevalent types of fraud businesses, organizations, and government agencies experience are:

- **Account Takeover Fraud (ATO) -** ATO occurs when a cybercriminal gains access to a victim's login credentials to steal funds or information typically via password-based attacks including brute force, rainbow table attacks, credential stuffing, phishing, and malware. ATO is one of the top threats to financial institutions and their customers due to the financial losses and mitigation efforts involved.
- **New Account Fraud (NAF)** - also called Account Opening (AO) Fraud, often happens as a result of using stolen identities or assemblages of personal information to create a synthetic digital ID and can be more difficult to detect but has advantages for attackers. This type of fraud involves gathering complete sets or bits of PII (Personally Identifiable Information) on legitimate persons to construct illegitimate accounts.
- **SIM Swap Fraud** - This type of fraud exploits a weakness in two-factor authentication and two-step verification in which the second factor is a text message (SMS) or a call made to a mobile phone. In this sense, it is a special kind of ATO fraud that relies upon social engineering and/or insider fraud.

In today's digital age, businesses must be able to identify their customers from fraudsters or they will not only risk financial loss but also lose their customer's trust. The fact that password reuse is a common practice among customers only exacerbates the problem. To tackle this problem, increasing identity and authentication assurance at registration and authentication time is fundamental.

This entails moving away from authentication with shared secrets, such as passwords, which accounted for 89% of web application breaches, and phishable factors, such as OTPs and push notifications. Therefore, the solution is to get rid of the password from the customer experience and the database so that it is never used or stored. Plus, authentication can only be secured with factors that cannot be phished or intercepted via man-in-the-middle (MitM) attacks.

If successfully implemented, a passwordless MFA solution will eliminate account takeover fraud and improve the overall security of your organization.

To understand why a passwordless solution has the potential to prevent fraud and enhance the IT systems of an organization, it is important to first differentiate between the offerings in the market. Many solutions claiming to be passwordless do not entirely eliminate passwords, but simply reduce the number of passwords implemented or add another insecure factor for authentication. Various solutions are still password-bound such as password managers, and MFA solutions that utilize passwords as a factor in their authentication and/or recovery process.

Passwordless authentication solutions should provide a consistent login experience across all devices, introduce a frictionless user experience, and get rid of the dependence on passwords or other easily phishable factors. For this reason, selecting the right passwordless solution that meets the unique challenges and needs of each organization is essential. The passwordless journey must take into account the expectations of each of your organization's customer segments as well as the appropriate level of security to mitigate and prevent fraud.

4 Passwordless Authentication

Passwordless MFA solutions should be able to eliminate the reliance on passwords, or other easily phishable factors, as authentication methods. Replacing legacy MFA with passwordless MFA solutions might make all the difference between surviving in a rapidly changing world and protecting your customers from fraud and credential theft.

Passwords are a known security vulnerability and, as a result, there have been a few key developments within the cybersecurity industry to resolve this issue to help organizations and consumers improve their security.

As a response to the over-reliance on passwords, the non-profit organization FIDO ("Fast IDentity Online") Alliance was launched in 2013 to develop and promote authentication standards. Over 40 organizations from various industries, including finance and technology, are represented on the FIDO Alliance\'s board of directors. The FIDO Alliance aims to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering usernames and passwords.

With the help of the FIDO Alliance, a set of open, scalable, and interoperable specifications has been developed to replace passwords as a secure authentication method for online services that are intended to support the following objectives:

- Support strong, multi-factor authentication.
- Enable selection of the authentication mechanism by both the end user and the Relying Party.
- Facilitate integration of new authentication capabilities.
- Complement existing single sign-on, and federation initiatives such as OpenID, OAuth, and SAML.
- Preserve the privacy of the end user.
- Provide frictionless and unified end-user experiences across all platforms and across similar Authenticators.

Furthermore, the FIDO Universal Authentication Framework (UAF) protocol supports authentication by a user without the use of a password. As a result of such developments, the market has seen an increase in passwordless authentication offerings over the past few years. Compared to traditional 2FA and MFA, passwordless solutions have proven to be a very simple and safe alternative.

If organizations are determined to eliminate passwords and the associated risk, they must adopt existing technologies that already enable it, or at least acquire the skills to take advantage of technological changes *within the industry.*

Traditional MFA solutions were supposed to overcome the issue of passwords. However, the problem is that some MFA solutions still rely on a password as the first factor of authentication. To make matters worse, the second factor is also often vulnerable to phishing attacks. In this case, OTPs and push notifications that pretend to be security prompts can be used to trick users into giving their account details to attackers.

As with passwords, these \"one-time codes\" can be stolen and misused. Attackers with access to a user\'s email or SMS can hijack the OTPs generated through 2FA and MFA solutions. In addition, legacy 2FA and MFA are challenging to set up and add friction to every login, which creates inconvenience for customers and users.

Therefore, to increase security and convenience, passwordless solutions should be able to support Risk-based Authentication (RBA). With RBA, data is continuously collected around the risk signals of the user and the device, while appropriate authentication is orchestrated based on those risk signals. The objective of continuous authentication for customers is to secure access to corporate resources across all endpoints and make better access decisions.

5 Risk-Based Authentication

By eliminating passwords completely and adopting a passwordless solution that supports risk-based authentication (RBA) by default without adding friction for customers, organizations will have the ability to improve both user convenience and security at the same time.

With businesses onboarding more remote employees, customers, and other external users, the volume of people needing access to critical data and systems increases exponentially. Given the surging demands of businesses and the need to provide better security, many organizations must implement RBA solutions to augment IAM systems if they have not already to help reduce the risk of fraud and data loss.

Risk-based authentication is an authentication method that analyzes the required authentication context of a user requesting access to a system in order to determine the risk associated with that transaction. For example, by taking a look at whether the user's device requires a passcode or biometric authentication, whether it is rooted or jailbroken, and whether the application and operating system are up to date.

Risk-based MFA can eliminate a substantial portion of ATOs by increasing authentication assurance levels. Risk-based MFA often evaluates credential intelligence, device intelligence, user behavioral analytics, and behavioral/passive biometrics.

Passwordless authentication solutions that support risk-based authentication mechanisms have the ability to increase the level of verification required for a customer to log in to an application or service, depending on the context of the login.

Evaluation of various factors at runtime or transaction time, according to customer set policies, to determine if transactions should proceed require additional attributes to be collected or denied. Examples of data points often considered in adaptive authentication and authorization scenarios include, but are not limited to:

- Geo-location
- Geo-velocity
- IP address
- User attributes
- User behavioral analysis
- Device identity and/or fingerprint
- Device hygiene

- Device reputation

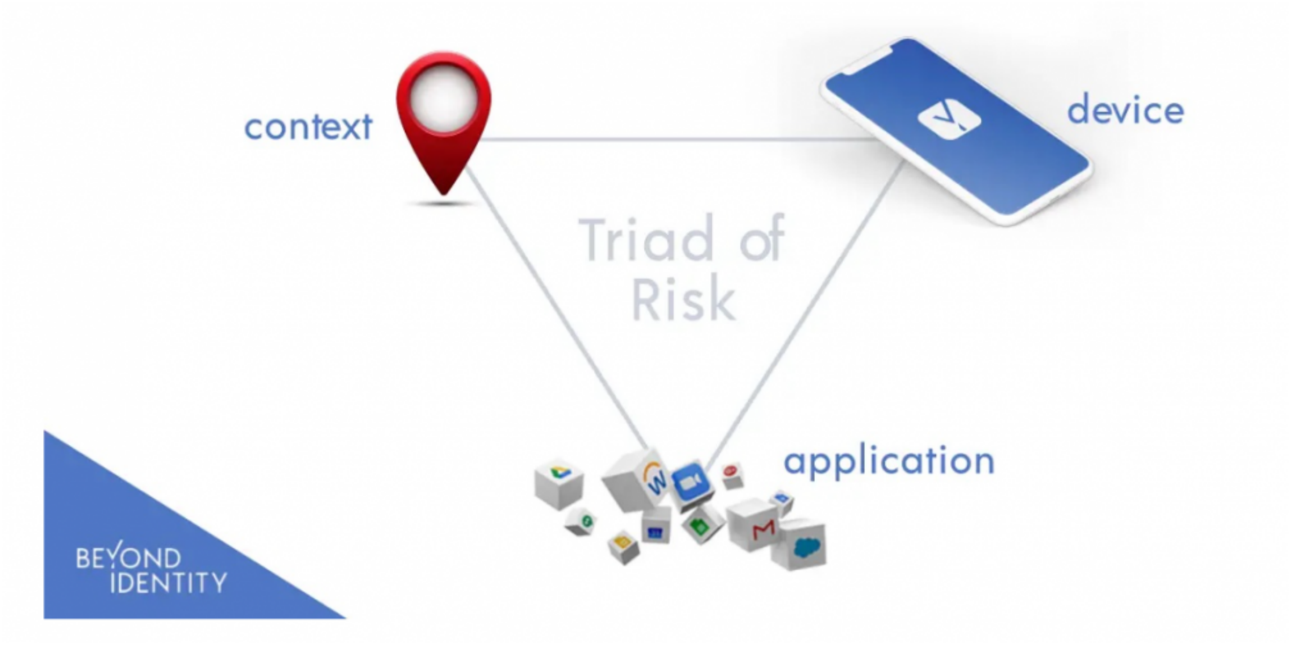

Figure 1: The triad of risk of Beyond Identity [Provided by Beyond Identity]

Based on the risk assessment, a decision is made as to whether the device is secure enough to access the desired level of functionality. This type of solution is being used today by enterprises to provide additional authentication assurance for access to applications involving health care, insurance, travel, aerospace, defense, government, manufacturing, and retail.

The ability to continuously evaluate various factors in a seamless manner at the exact time of authentication and continuously during an authenticated session can help protect organizations against fraud and credential theft. Furthermore, it protects the customer's privacy without causing significant friction to the user experience.

In the end, organizations need to find a passwordless authentication solution that provides customers with a frictionless user experience while maintaining security at the same time. Risk-based authentication ensures that only authorized users and devices that meet your security model can access company data and resources. Therefore, it is important that the authentication flow is not simplified and made easy at the expense of security.

6 Beyond Identity's Passwordless Authentication for Customers

Beyond Identity's Secure Customers delivers a passwordless MFA solution that protects customers against account takeover fraud and credential theft by eliminating passwords and other phishable factors.

Headquartered in New York City, Beyond Identity aims to lay the foundation of a passwordless future. Secure Customers is their newest product which provides companies with the ability to protect customer's data and privacy by eradicating passwords and delivering a passwordless MFA with only strong factors. Through Beyond Identity's cloud-native solution, customers can achieve complete passwordless identity management, increase security and convenience, and implement new business models.

Secure Customers, launched in September 2021, is a cross-platform passwordless authentication solution that allows businesses and organizations to provide consumers with a frictionless authentication experience without passwords, push notifications, one-time codes, and second devices for native mobile and web applications. Secure Customers offers a broad range of capabilities including the ability to protect customer's data, secure customer's accounts, and implement adaptive access control.

With support for open standards and robust documentation, integration is simple and requires minimal engineering resources. Secure Customers is deployed through embeddable SDKs in popular languages for iOS, Android, and web. This allows companies to deliver a branded first-party native experience to accelerate account creations, purchase completions, logins, and recovery while providing protection from account takeover fraud.

Beyond Identity allows companies to implement strong authentication from multiple devices based on public-private key pairs. All keys are cryptographically linked to the user and can be centrally managed using APIs. Instead of shared secrets, Beyond Identity authenticates customers with two strong factors - "something you are" from the device biometric and "something you own" from the private key - without requiring a second device for browser and native app authentication.

Upon registration, the user receives a binding token that prompts the creation of a unique, device-bound credential with a private key generated and stored in the Trusted Platform Module (TPM) or other secure element, depending on the technical platform, and a public key sent to the Beyond Identity Cloud. This binding token can be delivered via a variety of methods including email or in-app depending on the appropriate user workflows per company requirements.

During authentication, Beyond Identity issues a challenge signed by the private keys in the device's hardware TPM and makes a risk-based access decision based on security requirements. The solution acts on customizable risk signals from the user and their device's security posture to check the device's model, jailbroken status, TPM availability, password set, biometric set, secure enclave, volume encryption, and other security requirements, etc.

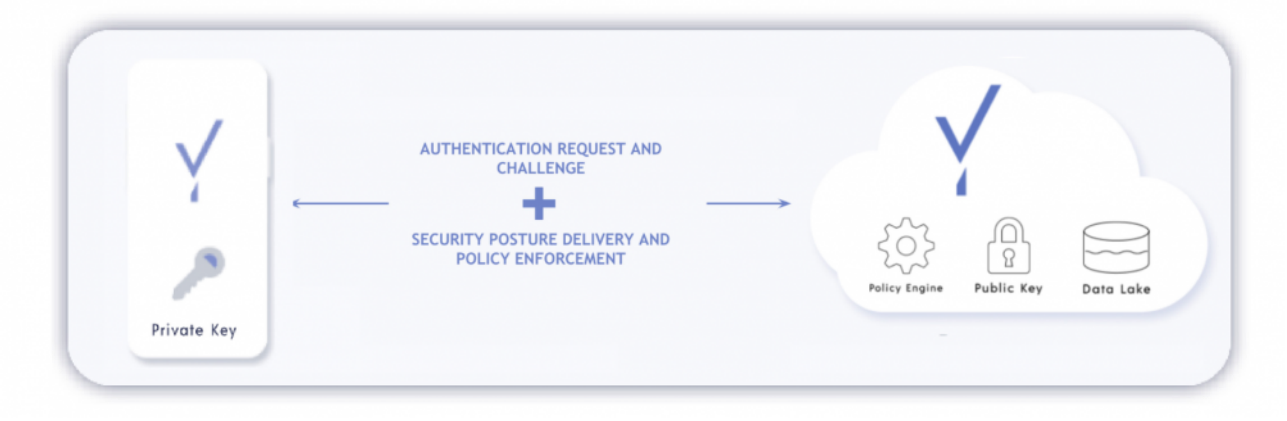
Private Key
AUTHENTICATION REQUEST AND CHALLENGE
+
SECURITY POSTURE DELIVERY AND POLICY ENFORCEMENT
Policy Engine
Public Key
Data Lake

Figure 2: The authentication flow of Beyond Identity Secure Customers [Provided by Beyond Identity]

Secure Customers provides an innovative implementation of asymmetric cryptography and TLS to remove passwords from the customer experience and the organization's database. As a result, there is no need for passwords, secondary devices for push notification approval or OTP completion, or separate authenticator applications. Using the self-signed X.509 certificate and the public-private key pairs ensures that users are in possession of only two attributes: "something you are" from the device biometric and "something you own" from the possession of a private key.

The benefits of Secure Customers include:

- Zero-friction, unphishable passwordless MFA
- Massive risk reduction
- Eliminate help desk calls and user downtime related to resetting passwords
- Compliance with PSD2 Strong Customer Authentication (SCA) standards
- Privacy-preserving credentials with tamper-resistant credentials backed by private keys
- A collection of SDKs in popular development languages
- Cross-platform support with native and web applications
- Leverages local device biometric (or fallback to local device PIN)
- Strong authentication with public-private key pairs and the use of asymmetric cryptography
- Makes account takeover fraud difficult by removing passwords from customer experience
- Ability to continuously collect the risk signals of the user and the device with risk-based authentication
- Adaptive step-up authentication based on real-time user and device risk via configurable security policies
- OAuth 2.0 and OIDC protocols with downstream support for SAML for Single Sign-On (SSO)

Furthermore, Secure Customers can embed self-service device and credential management (add device, delete credential, see credential information) within their application. It offers SCIM for bulk user and incremental provisioning as well as discrete API endpoints for user management.

The platform is also cloud-native with a 99.95% uptime SLA, global data centers, and has been stress tested to handle enterprise workloads and usage spikes. It integrates easily with a variety of Access Management solutions including Okta, Auth0, Keycloak, Curity, Ping Identity, ForgeRock, Microsoft Azure AD, and Microsoft ADFS (for on-prem or hybrid deployments).

In order to prevent ATO fraud, Secure Customers delivers a solution that makes it easier for customers to register without creating yet another password, using phishable factors like OTPs and push notifications, or picking up a second device. As a result, passwordless enrollment happens once and the only thing customers have to do is provide their email address to bind their identity to their device. This provides a safe, zero-friction, passwordless MFA that eliminates account takeover fraud and enhances the security of your organization.

7 Recommendations

To combat account takeover and other types of fraud, organizations must move away from passwords and replace them with strong passwordless multi-factor authentication solutions. Done right, organizations will increase both security and make authenticating more convenient for users. Furthermore, organizations will be able to protect customer's data and make sure that only allowed customers have access to the right information and resources. Only then will passwordless authentication meet customers' expectations and become a cornerstone of zero trust approaches.

While there are many things to consider, there are some key recommendations:

- **Define your organization's requirements**: It is important to determine the business needs of your organization and define them in a measurable way.
- **Follow a zero trust path**: Create a logical architecture that unifies different services and provides the capabilities your enterprise needs by aligning these defined requirements to a zero trust model.
- **Implement a phased implementation approach**: Take the necessary steps that better suit your business model by replacing legacy MFA providers with passwordless, invisible, and unphishable authentication solutions.
- **Understand your customers' needs:** In order to be able to meet customers' expectations, it is crucial to find out the challenges that customers face with existing solutions.
- **Select a deployment model:** Make sure that the solution you decide to incorporate into your organization supports your requirements, specifically the elasticity and scale required for supporting digital services.

Ultimately, embarking on a passwordless journey depends on your business model and requirements. Therefore, look for trusted advisors and competent vendors that will support you along your mission. Be sure to define the business requirements in measurable terms and to understand them.

8 Related Research

Leadership Compass Consumer Authentication
Leadership Compass CIAM Platforms
Leadership Compass Fraud Reduction Intelligence Platforms
Leadership Compass Enterprise Authentication Solutions
Leadership Brief How to Get Rid of Passwords - Today

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.